(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 June 2005 (23.06.2005)

PCT

(10) International Publication Number
WO 2005/057321 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/KR2004/003212

(22) International Filing Date: 8 December 2004 (08.12.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10-2003-0088895
9 December 2003 (09.12.2003) KR
10-2004-0050346 30 June 2004 (30.06.2004) KR

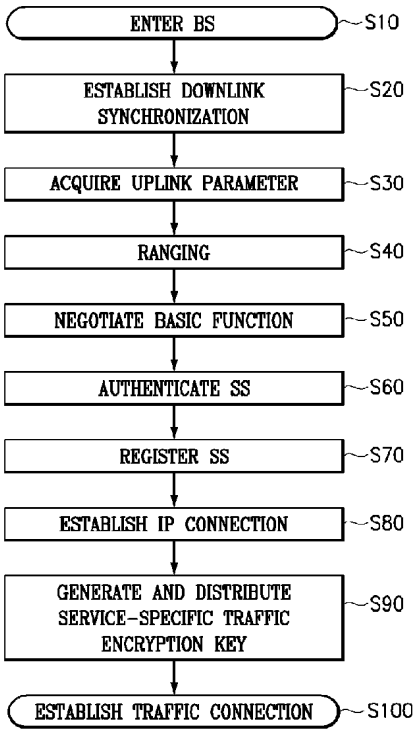
(71) Applicants *(for all designated States except US)*: **ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE** [KR/KR]; 161 Gajeong-dong, Yuseong-gu, Daejeon 305-350 (KR). **SAMSUNG ELECTRONICS CO., LTD.** [KR/KR]; 416 Maetan-dong, Yeongtong-gu, Suwon-si, Gyeonggi-do 442-742 (KR). **KT Corporation** [KR/KR]; 206 Jungja-dong, Bundang-gu, Seongnam-city, kyeongki-do, 463-711 (KR). **SK Telecom Co., Ltd.** [KR/KR]; 99 Seorin-dong, Jongro-gu, Seoul 110-110 (KR). **KTFREETEL CO., LTD.** [KR/KR]; 890-20 Daechi-dong, Gangnam-gu, Seoul 135-280 (KR). **HANARO TELECOM, INC.** [KR/KR]; Shindongah Fire & Marine Insurance Building 43, Taepyeongno 2-ga, Jung-gu, Seoul 100-733 (KR).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **CHO, Seok-Heon** [KR/KR]; 775-21 Shin-dong, Iksan-city, Jeollabuk-do 570-976 (KR). **PARK, Ae-Soon** [KR/KR]; Hanvit Apt. 138-301, Eoeun-dong, Yuseong-gu, Daejeon-city 305-755 (KR). **YOON, Chul-Sik** [KR/KR]; Seonkyeong Apt. 4-402, 255-1, Hagye-dong, Nowon-gu, Seoul 139-230 (KR). **KIM, Kyung-Soo** [KR/KR]; Hanul Apt. 109-1702, Shinseong-dong, Yuseong-gu, Daejeon-city 305-345 (KR). **AHN, Jee-Hwan** [KR/KR]; 149-7 Sinseong-dong, Yuseong-gu, Daejeon-city 305-345 (KR).

[Continued on next page]

(54) Title: METHOD FOR REQUESTING, GENERATING AND DISTRIBUTING SERVICE-SPECIFIC TRAFFIC ENCRYPTION KEY IN WIRELESS PORTABLE INTERNET SYSTEM, APPARATUS FOR THE SAME, AND PROTOCOL CONFIGURATION METHOD FOR THE SAME



(57) Abstract: Disclosed are a method for requesting, generating and distributing a service-specific traffic encryption key in a wireless portable Internet system, an apparatus for the same, and a protocol configuration method for the same. In the present invention, a subscriber station sends a Key Request message for requesting a service-specific traffic encryption key to the base station using a PKM-REQ MAC message, and a base station analyzes the Key Request message to generate the requested service-specific traffic encryption key. Subsequently, the base station sends a Key Reply message, including the generated service-specific traffic encryption key, to the subscriber station using a PKM-RSP MAC message. If the base station fails to generate the key, the base station sends a Key Reject message, including a reason for the failure, to the subscriber station.

WO 2005/057321 A2

(74) **Agent: YOU ME PATENT AND LAW FIRM**; Seolim Bldg., 649-10, Yoksam-dong, Kangnam-ku, Seoul 135-080 (KR).

(81) **Designated States** *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.